REMARKS

Claims remaining in the present application are numbered 1-25. Claim 10 has have been amended. No new material has been added as a result of the above amendments to the Claims.

CLAIM REJECTIONS

35 U.S.C. § 103(a)

Claims 1-5, 7-16, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al (6,696,490) in view of Rioz et al (WO 01/17310).

The rejection is respectfully traversed, for the reasons below. It is respectfully submitted that Claims 1-5, 7-16, 18 and 19 are patentable over Drummond in view of Rioz.

Claim 1 recites:

> A method for managing access to a network, comprising:
> providing wireless communication in a network;
> providing a firewall protection between said network and a wireless access device;
> submitting an identification code to said network from said wireless access device, said identification code associated with and pertaining to said wireless access device:
> determining the validity of said identification code;
> granting wireless network access to said wireless access device when said identification code is valid;
> denying wireless network access to said wireless access device when said identification code is not valid;
> issuing an alert when said identification code is not valid.

Accordingly, Applicants' invention is directed to wireless communication between a wireless access device and a network in which a firewall is disposed between the network and the wireless

access device. Further, Applicants' require an identification code related to the wireless access device to be submitted to the network for identification and access to the network.

The rejection states Drummond provides, in Figure 5, wireless communication in a network (120) in which a firewall (126) is between network (120) and a wireless access device, e.g., 136, 138, and 140. Applicants are unable to locate the firewall 126 between wireless access devices 136, 138 and 140 and wireless access point 124, as stated in the rejection.

As understood by Applicants, Drummond may suggest, in Figure 5, a wireless access point (wireless hub) 124 between a plurality of wireless access devices and an ATM 122. Drummond may also suggest, in Figure 5, a firewall (126) within the ATM 122. However, Drummond, as understood by Applicants, does not suggest a firewall disposed and operational at the location of the wireless hub 124.

Thus, Applicants respectfully assert that Drummond does not suggest or teach the limitation of "providing a firewall protection between said network and a wireless access device," as claimed.

The rejection further states that Drummond suggests (col. 6, line 61) submitting an identification code to the network from the wireless access device. As understood by Applicants, Drummond may suggest an identification code which can include a User ID and a password. Drummond may also suggest requiring additional user information that may include biometric inputs, digital certificates, or other user related information. Thus, as understood by Applicants,

Drummond suggests personal identification and values, e.g., user information, for authorization to access a network.

However, Applicants respectfully assert that Drummond does not suggest or teach the limitation of "submitting an identification code to said network from said wireless access device, said identification code associated with and pertaining to said wireless access device," as claimed.

The rejection states that Drummond (col. 6, lines 66-67) determines the validity of the identification code and grant access (col. 7, lines 1-2) when the identification code is valid. Applicants understand Drummond to suggest predicating authorization upon validity of user information compared to a database of authorized users and not predicating authorization upon validity of the identification code pertaining to the wireless access device, as claimed.

Therefore, Applicants respectfully assert that Drummond does not suggest or teach the limitation of "determining the validity of said identification code" in which the identification code pertains to the wireless access device, as claimed.

The rejection concedes, on page 5, that Drummond fails to disclose the limitations of "denying wireless network access to said wireless access device when said identification code is not valid" and "issuing an alert when said identification code is not valid." Moreover, Applicants respectfully submit that Drummond fails to teach or suggest these limitations.

The rejection further states that Rioz discloses (Figure 3, page 12, lines 2-5) denying wireless network access to said wireless access device when the identification code is not valid and further discloses (Figure 3, lines 5-7) issuing an alert when the identification code is not valid. Applicants respectfully assert that Drummond and Rioz, alone or in combination, fail to disclose or suggest this limitation.

Applicants understand Rioz to suggest (page 11, lines 13-30) an identification code that is predicated upon matching tokens in which an authenticating entity communicating with an authorization server via a secure packet data connection requests the authentication of the user trying to gain access. The authentication server provides the authentication entity with an authentication token. The authentication entity transmits the token to the remote host. The authentication server then contacts the mobile station and requests the user transmit the token sent to the remote host back to the authentication server from the mobile station. Thus, as understood by Applicants, Rioz suggests requiring a plurality of devices to obtain a token. As further understood by Applicants, Rioz may suggest the user input a PIN (personal identification number) before the user is able to send the token to the authentication server. Upon verification of the user PIN, the user may then transmit the token. Thus, as understood by Applicants, Rioz suggests an authorization based on a token that may be supplemented with a user PIN. However, as understood by Applicants, Rioz does not suggest or teach authentication predicated upon an identification code pertaining to a wireless access device, nor does Rios remedy the shortcomings of Drummond, as claimed.

Further, Applicants respectfully assert that Drummond in combination with Rioz fail to disclose the limitation of "denying wireless network access to said wireless access device when said

identification code is not valid" when the identification code pertains to the wireless access device as claimed.

Continuing, the rejection states that Rioz discloses issuing an alert when the identification code is not valid. As understood by Applicant and described above, Rioz issues an alert when the received token does not match the sent token. However, Rioz does not suggest or teach the limitation of "issuing an alert when said identification code is not valid" when the identification code pertains to the wireless access device, as claimed.

For the above reasonings, Applicants assert that the teachings of Rioz do not remedy the shortcomings of Drummond. Therefore, the combination of Drummond in view of Rioz fails to teach or suggest the claimed limitations of Claim 1.

Claim 2

The rejection states that Drummond discloses (Figure 5) the method wherein providing the wireless communication is accomplished with a wireless hub enabled for wireless communication. Applicants respectfully traverse the rejection for the reasons below.

Claim 2 recites:

> The method described in Claim 1, wherein said providing said wireless communication is accomplished with an intelligent concentrator enabled for wireless communication.

Applicants understand Drummond to suggest (Figure 5) a wireless access point (wireless hub) 124. However, Applicants are unable to locate within the cited reference that portion that discloses the claimed limitation of Claim 2.

Applicants assert that a wireless hub, as suggested by Drummond, and an intelligent concentrator, as claimed by Applicants, are not analogous. Those well versed in the art are cognizant that a hub is classified as a Layer 1 (physical layer) device in the OSI model. At the physical layer, hubs provide little or no support regarding sophisticated networking. Hubs do not read any data passing through them, they are unable to determine the data source or destination, and while they may possibly amplify the electrical signal they broadcast these packets out to all devices on the network - including the one that originally sent the packet. Thus, Drummond does not suggest or teach the limitations of Claim 2.

Claim 3

The rejection states that Drummond discloses (Figure 5, col. 7, lines 36-51) the method wherein providing the wireless communication is accomplished in circuitry resident in the wireless hub. Applicants respectfully traverse the rejection for the reasons presented below.

Claim 3 recites:

> The method described in Claim 2, wherein said providing said wireless communication is accomplished in circuitry resident in said intelligent concentrator.

Applicants understand Drummond to suggest a plurality of wireless interfaces, (Figure 5, col. 7, lines 36-51) including IEEE802.11, Bluetooth, IR, RF or other wireless interface, that

may be implemented to provide wireless communication. However, while Drummond may suggest wireless communication via a wireless hub, Applicants are unable to locate that portion of the cited reference that discloses the limitations of Claim 3. As such, Applicants respectfully assert that Drummond does not suggest or teach an intelligent concentrator nor does Drummond suggest or teach wireless circuitry resident in an intelligent concentrator. Therefore, Applicants respectfully assert that Drummond does not disclose the limitations of Claim 3.

Claim 4

The rejection states that Drummond discloses (col. 6, line66 to col. 7, line 1) the method wherein the authentication code is the media access number (User ID, password) of the wireless access device. Applicants respectfully traverse the rejection for the reasons presented below.

Claim 4 recites:

> The method described in Claim 2, wherein said identification code is the media access control number of said wireless device.

As understood by Applicant, Drummond suggests a User ID and further suggests a password both of which are compared to a database containing authorized users. Therefore, Applicants assert that Drummond suggests user-based authorization and not wireless access device identification as claimed. Therefore, Applicants respectfully assert that Drummond does not disclose the limitations of Claim 4.

Claim 5

The rejection states that Drummond discloses (Figure 5, identifying devices) the method wherein the determining the validity of the identification code is accomplished by reference to a list of valid identification codes. Applicants respectfully traverse the rejection for the reasons presented below.

Claim 5 recites:

> The method described in Claim 1, wherein said determining said validity of said identification code is accomplished by reference to a list of valid identification codes.

As understood by Applicant, Drummond suggests (Figure 5) identifying devices, e.g., a Biometric Scanner (fingerprints, retinal scan), a card reader (similar to inserting your Bank card into an ATM), or a Face/Voice Recognition System, that may be used in conjunction with user identification and/or authorization. Thus, as understood by Applicant, Drummond suggests user information and/or data upon which identification is based.

However, Drummond does not suggest an identification code based on the wireless access device nor does Drummond suggest storing identification codes that are based on and which pertain to a wireless access device. Therefore, Applicants respectfully assert that Drummond does not suggest or teach the limitations of Claim 5.

Claim 7

The rejection states that Drummond discloses (Figure 5) the method wherein the list of valid identification codes is resident in a server in the network. Applicants respectfully traverse the rejection for the reasons presented below.

Claim 7 recites:

> The method described in Claim 5, wherein said list of valid identification codes is resident in a server in said network.

As understood by Applicant, Drummond suggests (Figure 5) an identification code that is based on user information, e.g. User ID, password, a Biometric Scanner (fingerprints, retinal scan), a card reader (similar to inserting your Bank card into an ATM), or a Face/Voice Recognition System, that may be used in conjunction with user identification and/or authorization. Thus, as understood by Applicant, Drummond suggests user information and/or data upon which identification is based. While Drummond may suggest storing identification codes on a server, Drummond suggests storing identification codes containing user-based information upon which the identification is determined.

However, Applicants respectfully assert that Drummond does not suggest or teach the limitations of Claim 7 in which valid identification codes, based upon information pertaining to a wireless access device, can be stored in a server within the network.

Claim 8

The rejection states that Drummond discloses (Figures 4 and 5, col. 6, line 18 to col. 7, line 22) the method wherein the denying of wireless access to the network is accomplished simultaneously with granting access to wireless access devices with valid identification codes. Applicants respectfully traverse the rejection for the reasons presented below.

The rejection further states, on page 3, that Drummond does not disclose denying access if the identification code is invalid. Although Drummond may suggest a function for checking error logs, Drummond, as understood by Applicants does not disclose denying access.

Claim 8 recites:

> The method described in Claim 1, wherein said denying said wireless access to said network is accomplished simultaneously with granting access to said wireless accesses devices with valid identification codes.

Applicants are unable to locate that portion within the cited reference that discloses denying access. Thus, Applicants respectfully assert that Drummond does not suggest or teach denying while simultaneously granting access and therefore Drummond does not suggest or teach the limitations of Claim 8.

Claim 9

The rejection states that Drummond suggests (Figure 5, 120) the method wherein the network is a wireless personal area network.

Claim 9 recites:

> The method described in Claim 1, wherein said network is a wireless personal area network.

While Drummond may suggest a wireless network, as understood by Applicants Drummond suggests a wireless hub as an access point to the network, which, as described above with reference to Claim 1, does not provide necessary functionality, as required by Applicant. Drummond further suggests that access is granted upon verified user identification,

whereas Applicants invention is directed to provide access to a network upon verified wireless access device identification.

Therefore, Applicants respectfully assert that Drummond does not suggest or teach the limitations of Claim 9.

Thus, Applicants respectfully assert that in light of the above presented arguments, Claim 1 is believed to be allowable over Drummond in view of Rioz. Therefore, as Claim 1 is believed to be allowance, dependent Clams 2-5 and 7-9 are also believed to be allowable.

Therefore, Applicants respectfully request that the rejections of Claims 1-5 and 7-9 be withdrawn, and Claims 1-5 and 7-9 be allowed.

Claims 10-16, 18 and 19

The Office action further states that Claims 10-16, 18 and 19 are rejected as being unpatentable over Drummond in view of Rioz. Examiner has used arguments similar to those arguments presented for Claims 1-5, and 7-9, above.

Currently amended Claim 10 recites:

> A computer network, comprising:
> a server;
> a wireless connection device communicatively coupled with said server;
> a wireless access device enabled to wirelessly submit an identification code to said wireless connection device, said identification code associated with and pertaining to said wireless access device; and
> a firewall communicatively coupled to said server and said wireless connection device, wherein said firewall is enabled to grant network access to

said wireless access device when said identification code is valid and to deny access to said network by said wireless access device and issue an alert when said identification code is not valid.

Thus, Applicants respectfully assert that currently amended Claim 10 recites limitations similar to those presented in Claims 1-5 and 7-9. Therefore, arguments presented above with regard to Claim 1 and dependent Claims 2-5 and 7-9 are applicable and as such are incorporated herein by reference.

Thus, Applicants respectfully assert that in light of the above presented arguments, Claim 10 is believed to be allowable over Drummond in view of Rioz. Therefore, as Claim 10 is believed to be allowance, dependent Clams 11-16, 18 and 19 are also believed to be allowable.

Therefore, Applicants respectfully request that the rejections of Claims 10-16, 18 and 19 be withdrawn, and Claims 1-5 and 7-9 be allowed.

Claims 20-23

Claims 20-23 are rejected under 35 U. S. C. 103(a) as being unpatentable over Drummond et al. (6, 796,490) in view of Janik (6,518,724). Applicants respectfully traverse the rejections in light of the arguments presented below.

Claim 20 recites:

An intelligent concentrator, comprising:
a housing;

a cable connector coupled to said housing and adapted to communicatively couple said intelligent concentrator to a network data cable;

electronic circuitry mounted in said housing enabled to wirelessly communicate with a wireless access device and a network; and

a distributed firewall resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device.

Drummond, as understood by Applicants and as discussed above with reference to Claim 1, may suggest a wireless hub 84/124 to connect a wireless access device to an ATM 82/122 having disposed therein a firewall 96/126.

However, as understood by Applicants, Drummond does not suggest or teach a firewall disposed in a wireless hub 84/124, nor does Drummond suggest electronic circuitry disposed in hub 84/124 enabled to control access to the network, as claimed.

Janik, as understood by Applicants, may suggest (Figure 21) a wall switch device to provide a display of information from a network or a wall switch device having a docking station incorporated therewith to enable wireless communication between the wall switch device, having a PDA inserted in the docking station, and a network via a wireless transceiver base 2110. As further understood by Applicants, Janik may suggest the transceiver base 2110 coupled to a gateway 2112. However, as understood by Applicants, Janik does not suggest or describe electronic circuitry disposed in the wireless transceiver base 2110 to control access to the network, as required in Claim 20.

Thus, as understood by Applicants, Drummond does not suggest or teach electronic circuitry in a wireless hub 84/124 for controlling access to a network. Rioz, as understood by Applicants, does not remedy the shortcomings of Drummond.

Applicants respectfully assert that Drummond in view of Janik, do not, alone or in combination, disclose the claimed limitations of Claim 20. As such, Applicants respectfully assert that Claim 20 is patentable over Drummond in view of Janik. Accordingly, Applicants respectfully request that the rejection of Claim 20 be withdrawn and Claim 20 be allowed.

As Claim 20 is believed to be allowable, Applicants respectfully assert that Claims 21-23 are therefore allowable. As such, Applicants respectfully request allowance of Claims 20-23.

Claims 6, 24 and 25

The rejection states that Drummond and Rioz does not disclose a list of ID code in the wireless hub. The rejection further states that Janik may suggest a list of valid identification codes is resident in switch device.

Janik, as understood by Applicants, may suggest (Figure 22, col. 11, lines 33-39) a valid identification code that may be resident in the switch device in which the identification code is relative to the switch device. However, Janik, as understood by Applicants, does not suggest or teach the limitation of Claim 6 which requires an identification code associated with and pertaining to the wireless access device.

Thus, Applicants respectfully assert that Janik does not suggest or teach the limitations of Claim 6. As such, Applicants respectfully request that the rejection of Claim 6 be withdrawn and Claim 6 be allowed.

Regarding Claims 24 and 25, as Applicants believe that Claim 20 is allowable and from which Claims 24 and 25 are dependent, Claims 24 and 25 are therefore also allowable. Applicants respectfully request that the rejections of Claims 24 and 25 be withdrawn and that Claims 24 and 25 be allowed.

Claim 17

As Claim 10 is believed by Applicants to be allowable and from which Claim 17 is dependent, Applicants respectfully request that the rejection of Claim 17 be withdrawn and Claim 17 be allowed.

CONCLUSION

For the above rationale, Applicants respectfully submit that the present invention as claimed is patentable over Drummond in view of Rioz in further view of Janik under 35 U.S.C. § 103(a). As such, Applicants respectfully request that the objections of Claims 1-5, 7-16, 18 and 19 and the rejections of Claims 20-23 and the rejections of Claims 6, 24 and 25 and the rejection of Claim 17 under 35 U.S.C. § 103(a) be withdrawn and Claims 1-25 be allowed.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional fees or apply any credits to our PTO deposit account No. 23-0085.

Respectfully submitted,

Wagner, Murabito & Hao LLP

Dated: 4/15/, 2005

John P. Wagner
Registration No. 35,398

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060